www.iup.edu/iupgencyber

JUNE 13 TO JUNE 17, 2016

IUP GENCYBER: CYBERSECURITY CAMP FOR MIDDLE AND HIGH SCHOOL STUDENTS

- Learn detailed information about cybersecurity
- Learn hacking defense techniques
- Acquire skills to land your dream job
- Do any of these topics interest you? Sign up today!

Through this opportunity, you will learn safe online behavior, increase knowledge of cyberspace, and explore cybersecurity careers.

Advantages

Offered at no cost!

Miniature computer for each participant!*

FREE lunch and afternoon snack!

Instruction and mentorship from IUP faculty and other experts!

Skills and knowledge for a growing career field!

Register NOW space is limited!

Location:

IUP Main Campus

Contact Info:

Waleed Farag, Ph.D.
Computer Science
farag@iup.edu
(724) 357-7995

Dighton M. Fiddner, Ph.D.
Political Science
fiddner@iup.edu
(724) 357-2290

*Program is contingent on funding released by NSA

www.iup.edu/iupgencyber

JUNE 13 TO JUNE 17, 2016

IUP GENCYBER: CYBERSECURITY CAMP FOR MIDDLE AND HIGH SCHOOL TEACHERS

- Learn detailed information about cybersecurity
- Learn about promising careers for students
- Acquire skills to change the future of your students
- Do any of these topics interest you? Sign up today!

Through this opportunity, you will learn safe online behavior, become part of the solution to the nation's shortage of skilled cybersecuity professionals, and help inspire young people to direct their talents to cybersecurity, a profession of critical importance to our nation's future

Advantages

Offered at no cost!

An iPad to take home for each participant!*

Act 48 Credits

FREE lunch and afternoon snack!

Mileage reimbursement for those who qualify

Multidisciplinary cybersecurity teaching skills, and modules to be used in the classroom!

Register NOW space is limited!

Location:

IUP Main Campus

Contact Info:

Waleed Farag, Ph.D.
Computer Science
farag@iup.edu
(724) 357-7995

Dighton M. Fiddner, Ph.D.
Political Science
fiddner@iup.edu
(724) 357-2290

*Program is contingent on funding released by NSA

ADVANTAGES FOR STUDENTS

- Offered at no cost!
- Miniature computer for each participant!
- FREE lunch and afternoon snack!
- Instruction and mentorship from IUP faculty and other experts!
- Skills and knowledge for a growing career field!

ADVANTAGES FOR TEACHERS

- Offered at no cost!
- An iPad to take home for each participant!*
- FREE lunch and afternoon snack!
- ACT 48 Credits
- Mileage reimbursement for those who qualify!
- Multidisciplinary cybersecurity teaching skills, and modules to be used in class!

HOW TO APPLY

Applications can be sent via e-mail, mail, fax or you can also apply online.

To apply online or download an application and view other important information, please visit:

www.iup.edu/iupgencyber/

Once paper application is completed, please send it and all required documents in one package to:

E-mail: gen-cyber@iup.edu
Fax: 724-357-2724
Mail: Computer Science Dept.
Stright Hall, Room 319
210 South Tenth St.
Indiana, PA 15705

CONTACT INFORMATION

Dr. Waleed Farag
Professor of Computer Science
E-mail: farag@iup.edu
Phone: 724-357-7995

Dr. Mac Fiddner
Associate Professor of Political Science
E-mail: fiddner@iup.edu
Phone: 724-357-2290

Proudly affilliated with

IUP NSF NSA GenCyber

SUMMER 2016

CYBER SECURITY CAMP

PRESENTED BY IUP AND NSA

IUP GENCYBER

SUMMER 2016 PROGRAM

Gen Cyber is a new national initiative that is supported by the National Science Foundation and the National Security Agency. This program has the following objectives:

- Increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation.
- Help all students understand correct and safe on-line behavior.
- Improve teaching methods for delivering cybersecurity content for K-12 curricula.

THE FUNDED GRANT

Under the leadership of Dr. Waleed Farag, grant PI, and Dr. Mac Fiddner, grant co-PI, IUP, along with a selected group of national universities, has been awarded funding to hold a combination summer camp for middle and high school students and teachers.

The funded project, titled "Fostering a Strong Cybersecurity Culture in High and Middle School Students and Teachers in Western PA through a Holistic Multidisciplinary Approach," proposes an interesting, novel, and multidisciplinary approach to foster interest in cybersecurity among middle and high school students and teachers in western Pennsylvania.

CAMP PROGRAM SUMMARY

This project will host a FREE (no cost to participants), five-weekday day-camp held June 13-17, 2016. Instruction will be delivered by a team of professors with numerous backgrounds but established expertise in cybersecurity teaching and research. Camp will include:

- An engaging content delivery approach that includes direct instruction, group activites, structured discover, and hands-on laboratory.
- 90 teaching hours proposed (30 for each group at a rate of six hours per day).
- 45 projected participants. 15 in each of the proposed cohorts (middle school, high school and teachers).
- Upon completion of camp, participants will have a strong understanding of cybersecurity in addition to mastering basic skills that help them be safer online.

CYBERSECURITY CAMP DAILY SCHEDULE

DAY 1 - JUNE 13, 2016

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Welcome, Introduction to team members, orientation and logistics HSS Building, Room 126		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Cybersecurity First Principles - Dr. Farag/Dr. Fiddner HSS Building, Room 126		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Facility tour, computer account access, equipment activation Stright Hall, Rooms 112 A, 112 B, 107 A		
11:50 a.m. to 1:00 p.m.	LUNCH - Stright Hall Rooms 112A/B		
1:00 p.m. to 1:50 p.m.	Session 2 - Facility tour, computer account access, equipment activation Stright Hall, Rooms 112 A, 112 B, 107 A		
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Introduction to Information Security Dr. Farag — Stright Room 107A	Session 1 - Social Media & Reputation Management Dr. Machado — Stright Room 112A	Session 1 - Basic Programming Dr. Pankaj/Dr. Rodger — Stright Room 112B
2:50 p.m. to 3:30 p.m.	BREAK - Stright Hall Rooms 112A/B		
3:30 p.m. to 4:30 p.m.	Session 2 - Introduction to Information Security Dr. Farag — Stright Room 107A	Session 2 - Social Media & Reputation Management Dr. Machado — Stright Room 112A	Session 2 - Basic Programming Dr. Pankaj/Dr. Rodger — Stright Room 112B

CYBERSECURITY CAMP DAILY SCHEDULE

DAY 2 - JUNE 14, 2016

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Basic Programming Dr. Pankaj/Dr. Rodger — Stright Room 112B	Session 1 - Introduction to Information Security Dr. Farag — Stright Room 107A	Session 1 - Social Media & Reputation Management Dr. Machado — Stright Room 112A
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Basic Programming Dr. Pankaj/Dr. Rodger — Stright Room 112B	Session 2 - Introduction to Information Security Dr. Farag — Stright Room 107A	Session 2 - Social Media & Reputation Management Dr. Machado — Stright Room 112A
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Social Media & Reputation Management Dr. Machado — Stright Room 112A	Session 1 - Basic Programming Dr. Pankaj/Dr. Rodger — Stright Room 112B	Session 1 - Introduction to Information Security Dr. Farag — Stright Room 107A
11:50 a.m. to 1:00 p.m.	LUNCH - Stright Hall Rooms 112A/B - CTC Guest Speaker		
1:00 p.m. to 1:50 p.m.	Session 2 - Social Media & Reputation Management Dr. Machado — Stright Room 112A	Session 2 - Basic Programming Dr. Pankaj/Dr. Rodger — Stright Room 112B	Session 2 - Introduction to Information Security Dr. Farag — Stright Room 107A
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Physical Security Dr. Giever — HSS Room 114	Session 1 - Secure Coding Dr. Farag — Stright Rooms 112B/107A	Session 1 - Networks/Smart Data Dr. Pankaj/Dr. Rodger — Stright Room 112A
2:50 p.m. to 3:30 p.m.	BREAK - Stright Hall Rooms 112A/B		
3:30 p.m. to 4:30 p.m.	Session 2 - Physical Security Dr. Giever — HSS Room 114	Session 2 - Secure Coding Dr. Farag — Stright Rooms 112B/107A	Session 2 - Networks/Smart Data Dr. Pankaj/Dr. Rodger — Stright Room 112A

CYBERSECURITY CAMP DAILY SCHEDULE

DAY 3 - JUNE 15, 2016

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Secure Coding Dr. Farag — Stright Rooms 112B/107A	Session 1 - Networks/Smart Data Dr. Pankaj/Dr. Rodger — Stright Room 112A	Session 1 - Physical Security Dr. Giever — HSS Room 114
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Secure Coding Dr. Farag — Stright Rooms 112B/107A	Session 2 - Networks/Smart Data Dr. Pankaj/Dr. Rodger — Stright Room 112A	Session 2 - Physical Security Dr. Giever — HSS Room 114
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Networks/Smart Data Dr. Pankaj/Dr. Rodger — Stright Room 112A	Session 1 - Physical Security Dr. Giever — HSS Room 114	Session 1 - Secure Coding Dr. Farag — Stright Rooms 112B/107A
11:50 a.m. to 1:00 p.m.	LUNCH - HSS Building Room 126 - RAND Guest Speaker		
1:00 p.m. to 1:50 p.m.	Session 2 - Networks/Smart Data Dr. Pankaj/Dr. Rodger — Stright Room 112A	Session 2 - Physical Security Dr. Giever — HSS Room 114	Session 2 - Secure Coding Dr. Farag — Stright Rooms 112B/107A
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Cyberbullies & Cyberpredators- Dr. Machado Stright Hall, Rooms 112A/B/C and 107A		
2:50 p.m. to 3:30 p.m.	BREAK - Stright Hall Room 112A/B		
3:30 p.m. to 4:30 p.m.	Session 2 - Cyberbullies & Cyberpredators - Dr. Machado Stright Hall, Rooms 112A/B/C and 107A		

CYBERSECURITY CAMP DAILY SCHEDULE

DAY 4 - JUNE 16, 2016

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Network Security Dr. Farag — Stright Room 107A	Session 1 - Database Vulnerabilities Dr. Smith — Stright Room 320	Session 1 - Insider Threats Dr. Gossett — Stright Rooms 327/329
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Network Security Dr. Farag — Stright Room 107A	Session 2 - Database Vulnerabilities Dr. Smith — Stright Room 320	Session 2 - Insider Threats Dr. Gossett — Stright Rooms 327/329
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Database Vulnerabilities Dr. Smith — Stright Room 320	Session 1 - Insider Threats Dr. Gossett — Stright Rooms 327/329	Session 1 - Network Security Dr. Farag — Stright Room 107A
11:50 a.m. to 1:00 p.m.	LUNCH - Stright Hall Room 112A/B		
1:00 p.m. to 1:50 p.m.	Session 2 - Database Vulnerabilities Dr. Smith — Stright Room 320	Session 2 - Insider Threats Dr. Gossett — Stright Rooms 327/329	Session 2 - Network Security Dr. Farag — Stright Room 107A
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Session 1 - Insider Threats Dr. Gossett — Stright Rooms 327/329	Session 1 - Network Security Dr. Farag — Stright Room 107A	Session 1 - Database Vulnerabilities Dr. Smith — Stright Room 320
2:50 p.m. to 3:30 p.m.	BREAK - Stright Hall Room 112A/B		
3:30 p.m. to 4:30 p.m.	Session 2 - Insider Threats Dr. Gossett — Stright Rooms 327/329	Session 2 - Network Security Dr. Farag — Stright Room 107A	Session 2 - Database Vulnerabilities Dr. Smith — Stright Room 320

CYBERSECURITY CAMP DAILY SCHEDULE — DAY 5 - JUNE 17, 2016

	Middle School Students	High School Students	Teachers
9:00 a.m. to 9:50 a.m.	Session 1 - Privacy - Dr. McDevitt Stright Hall, Rooms 112A/B/C and 107A		
9:50 a.m. to 10:00 a.m.	BREAK		
10:00 a.m. to 10:50 a.m.	Session 2 - Privacy - Dr. McDevitt Stright Hall, Rooms 112A/B/C and 107A		
10:50 a.m. to 11:00 a.m.	BREAK		
11:00 a.m. to 11:50 a.m.	Session 1 - Decision Making Simulation - Dr. Fiddner HSS Building, Rooms 103,104,117,124,125,126		
11:50 a.m. to 1:00 p.m.	LUNCH - HSS Building Room 126		
1:00 p.m. to 1:50 p.m.	Session 2 - Decision Making Simulation - Dr. Fiddner HSS Building, Rooms 103,104,117,124,125,126		
1:50 p.m. to 2:00 p.m.	BREAK		
2:00 p.m. to 2:50 p.m.	Finale Competition HSS Building, Room 126		
2:50 p.m. to 3:30 p.m.	BREAK - Stright Hall Rooms 112A/B		
3:30 p.m. to 4:30 p.m.	Post-camp Assessment/Conclusion Stright Hall Rooms 112A/B		

Introduction to Information Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #2: Explore the use of basics operating systems commands on different platforms.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #4: Least Privilege
- #5: Layering
- #7: Information Hiding

Description:

This module presents an easy-to-understand introduction to fundamentals of information security. Participants will learn about key information security concepts such as confidentiality, integrity, availability, and non-repudiation. Various components of a typical information system will be presented including software, hardware, data, people, etc. The module will highlight the importance of humans as a central component of any system and how human errors are typical causes of system compromises. The common saying that "humans are the weakest link of the security chain" will be expounded with several real-world examples. In such context, several security first principles will be fully explained. The concept of least privilege will be introduced as a technique that will help minimizing human errors or at least help containing the consequences of such errors. For example, assigning a regular user privileges to an employer (and not administrative access) will result in a much less catastrophic consequences of accidental deletion of a file or improper permission settings. Such errors will be contained by the limited access privileges given to the employer. Additionally, when discussing various components of an information system the concept of layering and defense-in-depth will yield themselves well. For example, the discussion will include an explanation of how various components can be viewed as various layers of security in which an attacker has to overcome this series of defensive layers in order to conduct a successful attack.

Moreover, different types of malicious software (malware) will be presented including viruses, worms, logic bombs, Trojan horses, and back doors. Various effective countermeasures will be expounded in details including the use of antimalware and antimalware while relating such use to some the first principles such as least privileges and layering. In addition, this module will discuss various security threats and attacks including software attacks, forces of nature and equipment malfunction. A considerable portion of this module is dedicated to a set of carefully chosen active learning simulations and hands-on activities in order to reinforce students' understanding of the covered topics and create a better engaging environment as described below.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include basics of Unix/Windows commands, name resolution service, network reconnaissance and enumeration tools, and password cracking tools. Another approach is to use mobile technology to maximize participant involvement through the use of their own smart phones (BYOD) and/or the provided mobile devices. Services such as tophat and Poll Everywhere are good candidates in such regards.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

The contents of the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how these security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as advanced operating systems use. The contents will also advance in the level of difficulty when being presented to the Middle school group compared to when being presented to the High school students.

How the Teachers and Students groups will be interacting:

This module will not have explicit interaction among the three groups. But, input from the teachers will be sought on how to better deliver the module contents to the other two students groups. Teachers and student groups will have plenty of chances to work and interact with each other in most of the first day's sessions, during the two working lunches facilitated by two invited guest speakers and during the merged cyberbullies sessions on Wednesday. We will also provide a very engaging, culminating, and competition-based activity that will involve all three groups in the last day of the camp. Such culminating activity will emphasize the 10 cybersecurity first principles.

Introduction to Network Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #3: Explain different types of attacks on computing systems.
- #4: Experiment with different tools and techniques used to attack and/or defend systems.
- #13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #1: Domain Separation
- #4: Least Privilege
- #5: Layering
- #7: Information Hiding
- #10: Minimization

Description:

This module will start by a brief review to the fundamental working principles of computer networks that were covered in the Networks/Smart Data module. Then, the participants will be introduced to various types of attackers and their varying motivation. The module will also discusses numerous malicious attacks including password guessing, man-in-the-middle, replay, session hijacking, and Denial of Service (DoS). In addition, various effective countermeasures will be expounded in details including the use of firewalls and intrusion prevention systems while relating such use to some the first principles such as layering and least privileges. Besides, the basic idea of encryption will be introduced and the role it plays in securing the information while in transit or in storage.

Moreover, the module will overview various categories of hackers and their motivations. In doing so, ethical concepts will be discussed including some of the controversies associated with various issues such as hacktivism. A considerable portion of this module is dedicated to a set of carefully chosen active learning simulations and hands-on activities in order to reinforce students' understanding of the covered topics and create a better engaging environment as described below One example of the interactive simulation used in this module is one that addresses how a real-world networking system such as email can be secured.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their

comprehension of taught contents. Such lab activities include network reconnaissance, password cracking tools, and traffic analysis. In addition, we are using a number of simulating activities that highly promote participants' engagement and make them positive contributors to the learning process. Another approach is to use mobile technology to maximize participant involvement through the use of their own smart phones (BYOD) and/or the provided mobile devices. Services such as, Kahoot, tophat and Poll Everywhere will be used to achieve this.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form an interactive quiz administered via online tool such as Kahoot and given towards the end of this module. Such environment promote competitiveness and encourage students to be involved. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

In this module, the examples used and scenarios presented will have difficulty levels suitable for each of the groups. For the teachers group, topics covered will stress how these fundamentals of secure programming can be integrated into the K-12 curriculum in addition to focusing on developing a sample lesson plan for one of the discussed topic. Moreover, the contents presented and programming source code used will advance in the level of difficulty when being presented to the Middle school group compared to when being presented to the High school students.

How the Teachers and Students groups will be interacting:

This module will not have explicit interaction among the three groups. But, input from the teachers will be sought on how to better deliver the module contents to the other two students groups. Teachers and student groups will have plenty of chances to work and interact with each other in most of the first day's sessions, during the two working lunches facilitated by two invited guest speakers and during the merged cyberbullies sessions on Wednesday. We will also provide a very engaging, culminating, and competition-based activity that will involve all three groups in the last day of the camp. Such culminating activity will emphasize the 10 cybersecurity first principles.

Introduction to Smart Data Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #7: Information Hiding

Description:

This module presents an easy-to-understand introduction to fundamentals of information security by utilizing a case study. Participants will learn about key information security concepts such as those listed below:

Smart Data (SD) analyzes data for a global market. Up to this point it has never had an information security department. They are hiring you as their first Information Security Manager. You must set up the department and make sure that SD is prepared to deal with the risks and challenges faced by the company. Please work in teams of two or three and look your answers up on the Internet. There may not be a "right" answer but as a manager you will face numerous options. Be prepared to justify your solution and explain why it is the best choice.

1. What are the immediate challenges that the company faces?
2. What are the challenges that you will face in your role as Security Manager?
3. Use the AIC triad and list some important security considerations that the company faces.
4. How important is Senior Management Support and why?
5. In your security plan, what should be addressed in the initial security statement?
6. How can you create a new security culture within SD?
7. What cultural problems are you going to face in establishing a security program?
8. What security concepts may be violated at SD currently that should be addressed?
9. There are many different operating systems being utilized; how will you address this problem?
10. What are the advantages and disadvantages of solving the multiple OS problem?
11. Define a procedure from a security perspective and describe the main intent.
12. What is a policy and how is it implemented?
13. From a HR perspective list some good practices related to hiring and firing.
14. What is the role of an information custodian?
15. What are the primary risks that you see as facing SD?
16. What are some sources of threats to SD?

17. What areas should be included in the ethics statement for SD, from a security perspective?

SD recently acquired a small company and their network has been pieced together from several initiatives. As security manager you must prepare a security review and recommend initiatives.

1. What is the primary security requirement of a network?
2. What are the main network security requirements?
3. What would be the benefits and security risks of a VOIP system to SD?
4. Why would SD decide to install Wireless Access Points (WAP)?
5. What precautions should be taken before installing WAP?
6. Define jitter, latency and Quality of Service (QoS).
7. If SD sets up a website to make payments directly, then what precautions need to be taken?
8. What is MLPS and what benefits and risks does it offer compared to a leased line solution?
9. How can SD obtain a QoS level that is better than a packet-switched network?
10. What are the two things that an analog signal varies?
11. How do you indicate the beginning and end of asynchronous communications?
12. What is the most reliable network structure?
13. What is radius and how is it used?
14. What is the most common method of providing secure communications?
15. What is the threat associated with DNS?
16. What are the major parts of SSL and TCP setups?
17. What are the three parts of Security Association?

learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include basics of Internet and IUP Library research on cybersecurity issues.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, peer-assessment, and constructive answers to the case questions. For example, a carefully chosen set of questions on the covered topics can form a case quiz given at the end of this module. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contributes to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how these security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as advanced operating systems use. The contents will also advance in the level of difficulty when being presented to the Middle school group compared to when being presented to the High school students.

How the Teachers and Students groups will be interacting:

This module will not have explicit interacting among the three groups. But, the contents covered in the teachers group will primarily focus of how to integrating these security concepts in the K-12 curriculum. Also, input from the teachers will be sought on how to better deliver the module contents to the other two students groups. We also are planning a culminating competition-based activity among all three groups towards the end of the camp.

Cybersecurity Decision Making Simulation

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3). This instructional module will provide the student with knowledge and praxis in:

1. Demonstrate substantial understanding of the cybersecurity first principles.
2. Explain different types of attacks on computing systems
3. Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.
4. Exemplify the ability to identify the authenticity and credibility of access requests.
5. Develop skills needed to defeat various mal- and social engineering attacks.
6. Apply the knowledge gained in solving real-world, scenario-based problems.
7. Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1). All of the Cybersecurity First Principles will be involved in developing policy options for the decision maker, but the following are specifically the ones most relevant to the teams' consideration:

#1 - Domain Separation: separate areas of control.

#2 - Process Isolation: separating processes in a system so that a problem in one does not affect any others

#4 – Least Privilege: allows the minimum number of privileges necessary to accomplish the task.

#6 – Abstraction: removes any clutter that can distract and possibly be used in an incorrect way and only provides the minimum information necessary to accomplish the task.

Description:

This decision making simulation addresses the least privilege, process isolation and abstraction first principles of security by illustrating the essential role and fallibility of the human user in cybersecurity. The exercise demonstrates the ambiguity of the origin and intention of interruption to and/or corruption of digital media using a simulated "real world" situation. Participants in the exercises take on the role of advisors to a senior-level decision-maker (Secretary of Defense) in a group deliberative process where the principal task is to finalize advice for a formal deliberative/decision-making meeting on recommendations for the President on possible short-term technical solutions to a set of pressing cyberspace security problems that emerge in the context of a future political-military crisis.

learner-centered classroom:

The camp participants will be divided into collaborative teams of teachers and students competing against each other to develop the best advice for the short-term technical solutions to the simulation's set of pressing cyberspace security problems. Each camp participant will be

provided major features of the international security environment, the infrastructure security environment, and a set of instructions the day before the simulation to familiarize them self with the situation at the beginning of the exercise. A situation report outlining a crisis will be given to each team at the start of the exercise for them to deliberate recommendations to the Secretary of Defense.

Assessment:

Each team of teachers and students will be provided an "adviser" to offer international security advice in their deliberations. At the conclusion of the exercise, each team will present their advice to the decision maker and the advisors will compare the character and results of their deliberations to determine their ranking.

Suitability to various groups:

The international security material in this module may be too advanced for middle school students but they should be able to participate fully given the material provided the day before the exercise and as part of the collaborative student-teacher structure of the simulation. Even though possibly introducing unfamiliar material, the high school students and teachers should be able to grasp it relatively quickly given the pre-simulation provided material.

How the Teachers and Students groups will be interacting:

It is envisioned that the students will have the most active role in the collaborative deliberations of the simulation. One should assume the role of the group's chair and organize the rest of the students to examine different aspects of the situation provided in the "situation report" that specifies the "crisis" to which they are responding. The teachers will serve as advisers to the students assigned to their groups and help direct the chair and other student participants in their assigned tasks.

Cyber Bullying and Cyber Predator Module

Developed by Crystal Machado, Melissa Calderon, and Abdulsalami Ibrahim

Module Learning Outcomes:

#1: Demonstrate substantial understanding of the cybersecurity first principles.

#5: Realize the importance of password and username management and apply effective approaches to increase their security.
#8: Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.
#10: Exemplify the ability to identify the authenticity and credibility of access requests.
#12: Apply the knowledge gained in solving real-world, scenario-based problems.
#13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

#4: Least Privilege
#5: Layering
#6: Abstraction
#7: Information Hiding
#9: Simplicity of Design
#10: Minimization

Description:

Cyberspace is an exciting place which offers people of all ages a host of learning opportunities. It is also home to cyber bullies and cyber predators who mask themselves, and maneuver without being seen. Cyber bullies intimidate others through email, instant messages, social media and websites. Some cyber predators look for sexual gratification, others seek personal gains which could be emotional, financial, or even for the purpose of immigration. This module will provide middle and high school students and teachers with information that will help them to recognize the dangers in cyberspace. It will provide them with the opportunity to listen to teens and young adults' real-life stories and provide them with resources, tools and strategies that can be used to avoid and/or combat these dangers.

Upon completion of the module middle and high school students and teachers will be able to :

- Define and describe the difference between cyber bullies and cyber predators
- Identify some of the dangers in cyberspace
- Assess the impacts of negative online behavior
- Identify ways to manage and prevent intended and unintended cyberbullying behavior
- Create a personal plan to act with resilience and self-awareness when online
- Empower peers with tools/resources and strategies that protect users against cyber dangers

Learner-Centered Classroom:

This module will be delivered by a team that includes a professor, a K-12 teacher/adjunct professor, and an international doctoral student. The team will create a highly interactive environment that provides students and teachers with an opportunity to interact with the content and each other. Instruction will include whole group activities as well as small group activities structured by level (middle school, high school, and teachers) and heterogeneous grouping across the three levels. The team will use direct instruction, structured discovery and informal instruction to deliver the content.

To help participants see the "person" behind statistics related death or victimization of children they will participate in an activity called "In the News: The Story behind the Face." Following a brief think-pair-share they will engage in a whole class discussion about the difference between cyber bullies and cyber predators. Participants will then be engaged in an interactive video story (Zaption or Nearpod). This will enable to (1) define and describe cyberbullying behavior (2) assess the impacts of negative online behavior (3) recognize the legal, social, emotional and ethical implications of cyber bullying (4) identify ways to manage and prevent cyberbullying behavior.

To provide participants with an opportunity to engage in "proactive" rather than "reactive" behavior, they will be given an opportunity to discuss:
(a) the Public Service Announcement created by Los Angeles-based non-profit dance company MusEffect 953K – Inspiring Action Against Cyberbullying which generated over 1.2 million views and inspirational stories of healing and resolution from audiences across the globe.
(b) and the forever free application Re-think Application which delays participants' messages from being sent in order to give them an opportunity to consider the consequences of the message and make a further determination as to whether they should send the message.

Finally, they will then, working in 5 heterogeneous small groups, create a one-page "Stall News" bulletin that targets the following groups: (a) Teachers (b) Middle Schoolers (c) High Schoolers (d) Principals (e) Parents.

Assessment:

A series of formative and summative assessments will be used during the module. The team will evaluate participants' ability to distinguish between creative and creepy, funny and offensive, personal and private through a series of informal assessments. These include a think-pair-share at the beginning of the session, participants oral reactions to the bar diagrams and qualitative scenario-based responses embedded in the Zaption, the whole group discussions related to making educated decisions, and engagement in the small group activity. Summative assessment will include a review of the one-page "Stall News" bulletin that each heterogeneous group team will present to the whole group at the end of the session.

Suitability to various groups:

This module will provide middle and high school students with an opportunity to interact and learn with and from teachers in a variety of ways. Both heterogeneous and homogenous grouping

will be used, based on the content and learning experiences, to ensure that the module appeals to the different groups. The content that is shared with each group will be age and interest appropriate.

How the Teachers and Students Groups will be Interacting:

Teachers and students will be interaction and learning from each other in a variety of ways. Both heterogeneous and homogenous grouping will be used during this module. Participants will engage in whole and small group discussions regarding personal consequences, decision-making, and use of resources for cyber security. Participants will be divided into heterogeneous groups and instructed to use a variety of resources on cyberbullying and cyber predators in order to create a one-page "Stall News" bulletin that targets a different group of stakeholders. Bulletins will be emailed to the team and shared with all groups at the end of the session.

Social Media and Reputation Management Module

Developed by Crystal Machado, Melissa Calderon, and Abdulsalami Ibrahim

Module Learning Outcomes:

#1: Demonstrate substantial understanding of the cybersecurity first principles.
#5: Realize the importance of password and username management and apply effective approaches to increase their security.
#8: Engage in scenario-based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place.
#9: Uncover their own digital footprint and learn how to give themselves an "online make-over."
#10: Exemplify the ability to identify the authenticity and credibility of access requests.
#12: Apply the knowledge gained in solving real-world, scenario-based problems.
#13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

#4: Least Privilege
#5: Layering
#6: Abstraction
#7: Information Hiding
#9: Simplicity of Design
#10: Minimization

Description:

Social media has gained considerable popularity with teens and young adults. While students have limited access to social media like Twitter, Facebook and Instagram at school, they often use social media to interact with peers and family members outside of the classroom. Students' and teachers' safety needs will be better served if they are informed about the ways in which these tools can be used in a safe and secure manner to provide opportunities for professional growth, enhanced home-school communication, and conversations that allow learning to continue beyond allotted class times.

This module will provide participants with an opportunity to engage in meaningful activities and discussions regarding the appropriate use of social media in order to build a strong positive online reputation. The team will collect quantitative data at the beginning and end of the session to examine the participants' prior knowledge as well as their understanding of the topic after the information has been presented. The team will deliver background information in a lecture/discussion based format regarding social media use by teens and adults. A demonstration

on how to perform a detailed name search will be provided by the team. The participants will then perform a name search while considering the items presented as ways to clean up their information and create a long-term positive online reputation. While managing their online reputation, participants will set up Google Alerts for their name and other items they wish to be alerted about through email. As a culminating activity, participants will demonstrate their knowledge of reputation management by creating a Public Service Announcement on the topic of online reputation management.

Upon completion of the module middle school and high school students and teachers will:

- Understand the positive and negative circumstances that can impact online reputations.
- Review and make appropriate changes to the personal information they have currently made available on social media sites.
- Have the ability to set-up monitoring alerts in order to manage their online reputation.
- Have demonstrate advocacy for the safe appropriate use of social media.

Learner-Centered Classroom:

This module will be delivered by a team that includes a professor, a K-12 teacher/adjunct professor, and an international doctoral student. The team will create a highly interactive environment that provides participants with an opportunity to collaborate while engaging in the content. Instruction will include whole group activities as well as small group activities structured by the participant's level of education (middle school, high school, and teachers). The team will use direct instruction, discussion, structured discovery, and informal instruction to deliver the content and learning experiences related to social media and online reputation management.

During the lab component of this session, participants will actively uncover their own digital footprint. They will examine ways to eliminate items that may have a negative impact while brainstorming and applying ways to enhance a positive online reputation. Participants will select a series of Google Alerts based on their personal needs and examine circumstances that warrant an email alert. In the end of the session, participants will collaborate in groups of two or three while creating a video recorded Public Service Announcement based on the items they personally feel are the most important to mention while creating an awareness of online reputation management. The diversity in these activities enables the team to create a learner-centered classroom where students are personally invested in the learning experience.

Assessment:

A series of formative and summative assessments will be used during the module. The game-based learning platform Kahoot will be used to survey participants' social media usage and knowledge of online reputation management practices. Participants also will create several Google Alerts and share the selected alerts with the other participants in the classroom. The use of this verbal assessment enables the team to evaluate that participants have successfully completed the task. Additionally, the sharing of information such as personally selected alerts

may provide beneficial ideas for other participants in the class. Participants will also work in small groups of two or three while creating a short 1 – 2 minute video recorded Public Service Announcement regarding social media and online reputation management. Each group's PSA will be emailed to the team and presented in the final discussion at the end of the session.

Suitability to various groups:

This module will provide participants in each cohort (middle school high school, and teachers) with an opportunity to interact with peers of other school districts. While the instructional methods are the same, for each group, the content for the different groups will be age and interest appropriate.

How the Teachers and Students groups will be interacting:

Given that age difference and level of access to social media that each group has, each cohort (middle school, high school, and teachers) will work independent of each other. The insights that are gained from each group, as well as the material they create will be shared with the group that follows. For example, the high schoolers will react to the Public Service Announcement created by the middle schoolers. The teachers will create a Public Service Announcement to assist other teachers in building pedagogy derived from examining the content created by the middle and high school students.

Insider Threats: Factors and Responses

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #3: Explain different types of attacks on computer systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security
- #11: Develop skills needed to defeat various mal- and social engineering attacks.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module Addresses the Following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #4: Least Privilege
- #7: Information Hiding
- Ethics

Description:

This module focuses on insider threats and their role in developing effective cybersecurity systems. Humans are the weakest link in cyber security and this will be exemplified in this module. Specifically, this module defines insider threats (versus errors), discusses characteristics of becoming a threat, examples of used threats, and how to prevent the damage caused by this group. The context of this discuss meets the least privilege cyber security principle, as well as ethical considerations.

The module will begin with a discussion of defining a crime and whether or not employees can commit crimes, though businesses tend to focus on the 'stranger' or customer committing a crime, such as stealing. Specific 'real life' examples will be provided with every point, such as employee theft examples with Walmart and UPMC. Discussion will address factors and motivations (i.e. criminological theories) in why employees would 'steal' from their employer, as well as tactics they have used in past events. Known risks factors provided by various federal and private agencies will be discussed and analyzed in possible prevention techniques. Least privilege will be discussed as a viable tactic to limit insider threats, as well as other mechanisms.

Learner-Centered Classroom:

This module is relevant to K-12 teachers, as their co-workers can be potential insider threats that impact their grading, curriculum plans, websites, personnel files, and other significant information. Various scenarios focused on K-12 issues for teachers will be provided for discussion, such as hiring protocols, computer access in school, sharing of password with co-workers and students, leaving computer unattended, and other events. Small group discussion will ensue with these scenarios that will lead to application of possible prevention techniques currently used and those that may need to be considered in the future.

In discussing insider threats with middle to high school aged students, scenarios will also be provided, though designed for relevance in their experiences, for small group discussions. Events such that can occur at home, school or place of employment will be addressed. Motivations and outcomes of security breaches will be discussed in relation to prevention. For example, if they know a student who works closely with a teacher and has the teacher's password and plans to look at an exam, what should the student do? Online video examples will also be used in showing the 'costs and damage' of these actions, which are provided by CERT.

Assessment:

For both teachers and students, a quiz will be given to them at the beginning of the session (pre), as well as at end (post), to gauge what they have learned about insider threats. Another tool used to assess their learning is a small group project. The groups will provide a 'real' scenario of an insider threat situation and outcome. The event, characters, location, security threat technique, and outcome will be developed and shown to the entire group as a performance that will be evaluated by the audience. Key concepts will be portrayed in the small group project and a rubric will be given to everyone to evaluate the group and for the groups to understand how they will be assessed.

Suitability to Various Groups:

The main concept and points in the understanding of insider threats are relate to all persons. The content will be adapted with relevant examples to students, as well as for teachers. Teachers will further understand the significance of their actions in the classroom, such as the potential threat when students share passwords with each other (or teachers to students) and allowing students to have full access to their computer system. Middle and high school students will understand the importance of following computer security protocols, such as not sharing passwords with others, and the significance of ethical decision making in having computer access beyond their home.

How the Teachers and Students Groups will be Interacting:

This module will have each group work independently to create a scenario where other groups will need to 'guess' who the insider threat is in the situation. The covered material will be the same for each group, though the scenario they devise will be unique to each group.

Introduction to Database Systems and Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

- #1: Demonstrate substantial understanding of the cybersecurity first principles.
- #2: Explore the use of basic operation systems commands on different platforms.
- #3: Explain different types of attacks on computing systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #7: Realize the importance of secure coding and apply effective techniques to improve security.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

- #1: Domain Separation
- #2: Process Isolation
- #3: Resource Encapsulation
- #4: Least Privilege
- #5: Layering
- #6: Abstraction
- #7: Information Hiding
- #8: Modularity

Description:

This module presents an easy-to-understand introduction to fundamentals of database systems and database security. Includes topics of information models, database schemas, basic CRUD operations, and SQL. Various database architectures from desktop only to multi-tier will be presented. Both graphical user interface and command line will be used to define, populate, query, and maintain a database. Security measures to define users and grant/revoke privileges on database objects will be covered along with roles of various users of database systems. SQL injection will be demonstrated together with a discussion of proper countermeasures. Includes a cursory discussion on stored procedures.

Learner-centered classroom:

This module is designed to be taught in an interactive environment in which all attendees will be active participants in the learning process. This module will first have the students implement a cash register system using MS-Access. After creating the system and populating the system with data, students will experiment with generating queries. All interactions with the system will use the graphical user interface of access. Subsequently, attendees will be introduced to Oracle using the command line interface. Pre-built SQL scripts will be used to build and populate a small database. Students will experiment with generating queries. The module will conclude with a hand-on demonstration of a web based database system which is vulnerable to SQL injection. Throughout the module security first principles will be emphasized.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. At the beginning of the module, attendees will asked as group to enumerate as cyber security first principles in general. At the end of the module attendees will be asked to again enumerate the cyber security principles, only this time emphasizing the relation to database systems. Both times this will be performed orally as a group. Experiments with database queries a means to explore use of basic operation systems commands on different platforms, and applying knowledge gained in solving real-world, scenario-based problems. Experiments with the vulnerable database system will realize the importance of secure coding and need for effective programming techniques to improve security A few pre/post camp questions will provide a degree of formal assessment.

Suitability to various groups:

The contents the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how the database systems can be integrated into the K-12 curriculum with emphasis on securing information stored in databases. The contents will also advance in the level of detail when being presented to the high school group compared to content being presented to the middle school students.

How the Teachers and Students groups will be interacting:

This module will not have explicit interaction amongst the three groups. Contents covered in the teachers group will primarily focus of how to integrating these security concepts in the K-12 curriculum, while those to students will focus on kindling their interest in the area of cybersecurity. Also, input from the teachers will be sought on how to better deliver the module contents to the other two students groups.

Physical Security Module

Module Learning Outcomes:

- #3: Explain different types of attacks on computing systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

- #4: Least Privilege
- #5: Layering
- #7: Information Hiding

Description:

This module on physical security addresses the cybersecurity threat from a more comprehensive standpoint. Students will be challenged to recognize and understand security concerns from multiple perspectives, ranging from the insider threat, outsider threat, to threats involving the actual physical components. Exposure to a design methodology, associated system components modules, and basic security principles are featured in this module. Students will also be exposed to the private and public responses to computer security problems, and introduced to a number of unique computer crimes and solutions to deal with these crimes. The importance of a sound security policy in the overall management of any organization is addressed.

Upon completion of the module students will:

- ❖ Possess an understanding of physical security system design and evaluation.
- ❖ Gain an understanding of the process of evaluating existing or proposed physical protection systems.
- ❖ Understand the policies and procedures needed to protect an organization and its computer resources from insiders who might do harm.
- ❖ Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

Learner-Centered Classroom:

In this module students will work as teams to test and develop an upgrade to an existing physical security system. Students will be challenged to upgrade a facility to increase its security posture. As part of this team building exercise students will test their upgrade using computer modeling software. A major component of this module will be the introduction of the design and evaluation process as developed by the Department of Energy. Students will be instructed on how to apply this process in their own protection and also the protection of personal assets such as a laptop or computer system. Students will be introduced to the three types of adversaries: outsiders, insiders, and outsiders in collusion with insiders, and the unique challenge each brings. They will also be exposed to the three basic tactics that adversaries might utilize: force, stealth, and deceit.

Assessment:

This module will be assessed by the following criteria - how realistic, budget and cost, probability of interruption from the modeling software, and upgraded policies and procedures. Each group will be challenged to develop an upgrade to a scenario and each group's upgraded will be assessed using a modeling program which assesses its ability to defeat an adversary.

Suitability to various groups:

The principles introduced in this module are applicable for all three groups. The development of sound protection policies and procedures are important for all individuals. Understanding how to model this process and gaining insight into the impact of changes to these policies and procedures will help both students and teachers alike in safeguarding themselves, not just in the cyber world, but in their day-to-day activities.

How the Teachers and Students groups will be interacting:

In this module each group will work independent of the others (middle school, high school, and teachers). The three groups will compete against each other on the best overall upgrade design. Each group will be exposed to the same material and will develop an upgrade to the same factitious facility.

Protecting Your Online Privacy

Module Learning Outcomes:

Participants will:

Consider the potential benefits and security risks of sharing information online

- Discuss the many ways that information is collected about us when we engage in online activities and what information is collected
- Discuss a variety of tools and techniques to that secure and protect online experiences
- Demonstrate knowledge of correct and safe online behaviors through successful completion of games and simulations
- Recognize the importance of password and username management and apply effective approaches to increase their security
- Engage in scenario based learning that allows them to make educated decisions and take deliberate action online to prevent things from going wrong in the first place
- Consider your online sharing practices and consider how to give themselves an online makeover
- identify the authenticity and credibility of access requests
- Develop skills needed to defeat various malware and social engineering attacks
- Realize the importance humans play in the digital world and understand how to minimize accidental and unintentional human errors
- Apply knowledge gained to the development of documents/activities designed to share online privacy preservation and safe computing practices

The Module addresses the following First Principles:

- Layering

Description

Computers are central to the daily lives of people of all ages and they allow us to do everything from keeping in touch with friends to finding information to filing our taxes and paying our bills.

Such technology is of great benefit, but it can also be risky. Unless you are aware of how this information gathering impacts your privacy, you are at risk of sharing sensitive information with scammers, hackers, and identity thieves.

This module will invite participants to consider how we share information every day though operations such as email, cell phone use, photo sharing and online shopping, GPS driving, online searching, and reading through real-life scenarios.

In the culminating session, which will follow, participants will work in groups to create a product or a plan to share what you have learned this week with students at your school.

Learner Centered Classroom

High school students and teachers will be briefly introduced to principles through active learning techniques including pre-and post-session polling, short engaging videos, hands on tutorials and games.

Assessment

Participants will be asked to engage with the material and each other frequently during the session. They will then play games in groups to practice principles presented. High school students will be asked to develop a learning document/activity demonstrating something they learned that they think is particularly important to their peers. Teachers will be asked to learning document/activity that teaches something about protecting privacy online that they think students in their classes would find engaging.

Suitability to Various Groups

Contents of the modules will be similar in topic but adapted for the different levels of learners. One of the 50 minute sessions will be offered simultaneously in two locations for students and a separate one for faculty). The second session will be developing and sharing learning documents/activities.

Teacher Student Interaction

Learning documents/activities will be shared by students and teachers will be during the second 50 minute session.

Lesson Plan

LESSON TITLE: Secure Coding

SUMMARY:

This module will build on the knowledge and skills gained via introducing participants to the "Java programming" module. In this module, participants will learn about the importance of secure programming and how they can apply simple, but effective techniques to make sure that their programs are more secure. For example, the concept of buffer overflow will be fully explained and used as an example of a very common security vulnerability that can be avoided by simply checking boundary conditions. Moreover, the concepts of input validation and black-box implementation will be introduced as other important approaches to ensure and improve the security of the coding process. One example

GRADE BAND:

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [x] High School

Time Required:

100.000 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

Activities in this module map directly to the following two outcomes proposed in our grant proposal:
1. Demonstrate in-depth understanding of the cybersecurity First Principles.
4. Have a better understanding of essential problem solving and programming concepts.
5. Apply programming knowledge and skills to design and implement reliable software systems that takes into account software assurance concepts.

Materials List:

Lab Computers
Eclipse IDE
.NET Visual Studio IDE
Lab Handouts

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Decribe the Teacher Instruction

-Discussion of secure coding basics
-Students will be involved in editing and running a number of Java and C++ programs
-Kahoot Quiz on programming basics
-Delivering customized modules to each group (more challenging labs will be given to high school students).

This lesson includes:

- [x] Mapping to Cyber Security First Principles
- [x] Learning Objectives
- [x] Assessments

Mapping to Cyber Security First Principles:

- [ ] **Domain Separation**
- [ ] **Process Isolation**
- [x] **Resource Encapsulation**
- [x] **Modularity**
- [x] **Least Privilege**
- [x] **Abstraction**
- [x] **Data Hiding**
- [x] **Layering**
- [x] **Simplicity**
- [ ] **Minimization**

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Project Writing Assignment Observation Walk Around Oral Questioning Other	Intro to secure coding presentation Instructor observation during group programming tasks Kahoot quiz

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

Description of Extension Activity(ies):

Acknowledgements: